

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-56473

(43) 公開日 平成10年(1998) 2月24日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 12/46  
12/28

識別記号

庁内整理番号

F I

H 0 4 L 11/00

技術表示箇所

3 1 0 C

審査請求 未請求 請求項の数32 O L (全 13 頁)

(21) 出願番号 特願平9-149743

(22) 出願日 平成9年(1997) 6月6日

(31) 優先権主張番号 特願平8-145854

(32) 優先日 平8(1996) 6月7日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 谷本 茂明

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 中島 彦之

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 磯田 邦彦

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74) 代理人 弁理士 志賀 正武

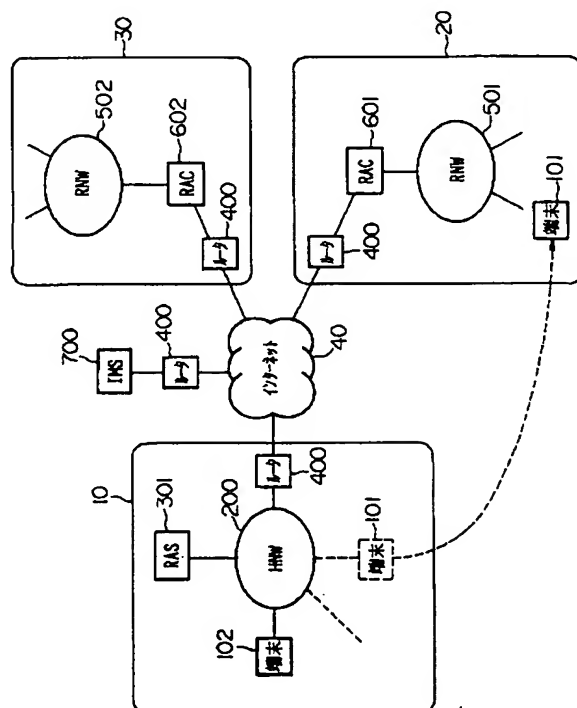
最終頁に続く

(54) 【発明の名称】 仮想LAN制御システム及び方法ならびに仮想LAN管理サーバ

(57) 【要約】

【課題】 端末離脱の検出を端末に特別なシステムや手順を設定することなく実現する。

【解決手段】 端末101がホームネットワーク200からリモートネットワーク501に移動して管理されている時、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワーク502に移動した場合の接続情報に基づき、端末とホームネットワークとのアクセスを制御するリモートアクセスサーバ301、リモートネットワークとインターネット40との通信を制御するリモートアクセスクライアント、端末の接続位置及びパケット送信を管理する仮想LAN管理サーバ700を用いて端末101の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行う。



## 1

## 【特許請求の範囲】

【請求項1】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANにおいて、

前記ホームネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、接続中の各端末の接続位置を示す管理テーブルを具備して、端末が前記リモートネットワークの1つに移動した時に、該端末と前記ホームネットワークとのアクセスを、該端末が前記ホームネットワーク内でアクセスしているかのように制御するリモートアクセスサーバと、

前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントと、

前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す管理テーブルを具備して、端末の接続位置及びパケット送信を管理する仮想LAN管理サーバとを有し、

いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、前記仮想LAN管理サーバを介して端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想LAN制御システム。

【請求項2】 前記端末離脱の検出において、各リモートアクセスクライアントは、接続中の前記端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシホールド値を超えた時に当該端末が離脱したと判定し、前記仮想LAN管理サーバに端末の離脱を通知することを特徴とする請求項1記載の端末離脱検出システム。

【請求項3】 前記リモートネットワークとして2つ以上のリモートネットワークが設けられており、前記端末離脱の検出において、端末が接続管理下の第1のリモートネットワークから第2のリモートネットワークに移動した場合、

該端末がパケットを送出すると、前記第2のリモートネットワークのリモートアクセスクライアントはこれを検出して端末が接続されたことを前記仮想LAN管理サーバに通知し、

## 2

通知を受けた前記仮想LAN管理サーバは、自身の管理テーブルを検索し、該端末がそれまで接続していたリモートネットワークが前記第1のリモートネットワークであることを認識し、該第1のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知することを特徴とする請求項1記載の端末離脱検出システム。

【請求項4】 前記端末離脱の検出において、前記リモートアクセスクライアントが自身の管理テーブルに記録された接続中の各端末に対して所定時間毎に監視メッセージを送信し、ある当該端末から応答メッセージが返送されない場合に当該端末が離脱したと判定し、前記仮想LAN管理サーバに端末の離脱を通知することを特徴とする請求項1記載の端末離脱検出システム。

【請求項5】 前記監視メッセージはOSIのレイヤ3アドレスを含み、前記応答メッセージはOSIのレイヤ2アドレスを含むことを特徴とする請求項4記載の端末離脱検出システム。

【請求項6】 前記端末離脱が検出されると、端末が離脱したリモートネットワークのリモートアクセスクライアントは、自身の管理テーブルの当該端末に関する情報を削除することを特徴とする請求項1記載の端末離脱検出システム。

【請求項7】 前記端末離脱が検出されると、前記仮想LAN管理サーバは、自身の管理テーブルの内容を更新するとともに、前記リモートアクセスサーバに端末の離脱を通知し、

通知を受けた前記リモートアクセスサーバは、自身の管理テーブルの内容を更新することを特徴とする請求項1記載の端末離脱検出システム。

【請求項8】 前記グローバル・ネットワークはインターネットであることを特徴とする請求項1～7いずれか記載の端末離脱検出システム。

【請求項9】 前記グローバル・ネットワークはイントラネットであることを特徴とする請求項1～7いずれか記載の端末離脱検出システム。

【請求項10】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANシステムにおける端末離脱検出方法であって、

いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする端末離脱検出方法。

【請求項11】 前記端末離脱の検出において、接続中の各端末がパケットを送出する毎に、自動的にタイマ値

## 3

が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシホールド値を超えた時に当該端末が離脱したと判定する請求項10記載の端末離脱検出方法。

【請求項12】 前記リモートネットワークとして2つ以上のリモートネットワークが設けられており、前記端末離脱の検出において、端末が接続管理下の第1のリモートネットワークから第2のリモートネットワークに移動した場合に、当該端末のパケットの送出を検出し、当該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第1のリモートネットワークであることを認識し、該第1のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知する請求項10記載の端末離脱検出方法。

【請求項13】 前記端末離脱の検出において、当該リモートネットワークに接続中の各端末に対して所定時間毎に監視メッセージを送信し、当該端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項10記載の端末離脱検出方法。

【請求項14】 前記監視メッセージはOSIのレイヤ3アドレスを含み、前記応答メッセージはOSIのレイヤ2アドレスを含むことを特徴とする請求項13記載の端末離脱検出方法。

【請求項15】 前記グローバル・ネットワークはインターネットであることを特徴とする請求項10～13いずれか記載の端末離脱検出方法。

【請求項16】 前記グローバル・ネットワークはイントラネットであることを特徴とする請求項10～13いずれか記載の端末離脱検出方法。

【請求項17】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANシステムで用いられる仮想LAN管理サーバであって、前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートネットワークのリモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す管理テーブルを具備して、端末の接続状態及びパケット送信を管理するものであり、

いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想LAN管理サーバ。

【請求項18】 前記仮想的なLANシステムには、前記リモートネットワークとして2つ以上のリモートネッ

## 4

トワークが設けられており、

前記端末離脱の検出において、端末が接続管理下の第1のリモートネットワークから第2のリモートネットワークに移動し、前記第2のリモートネットワークを介して本管理サーバに端末の接続が通知された場合、前記管理テーブルを検索し、該端末がそれまで接続していたリモートネットワークが前記第1のリモートネットワークであることを認識して該第1のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知することを特徴とする請求項17記載の仮想LAN管理サーバ。

【請求項19】 前記端末離脱が検出されると前記管理テーブルの内容を更新することを特徴とする請求項17記載の仮想LAN管理サーバ。

【請求項20】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANシステムで用いられる仮想LAN管理方法であって、

いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする仮想LAN管理方法。

【請求項21】 前記仮想的なLANシステムには、前記リモートネットワークとして2つ以上のリモートネットワークが設けられており、

前記端末離脱の検出において、端末が接続管理下の第1のリモートネットワークから第2のリモートネットワークに移動し、前記第2のリモートネットワークを介して端末の接続が通知された場合、該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第1のリモートネットワークであることを認識して該第1のリモートネットワークのクライアントに該端末の離脱を通知することを特徴とする請求項20記載の仮想LAN管理方法。

【請求項22】 コンピュータに請求項20または21記載の方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項23】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANシステムで用いられるリモートアクセスクライアントであって、前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの

通信を制御し、

いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とするリモートアクセスクライアント。

【請求項24】 前記端末離脱の検出において、接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時、当該端末が離脱したと判定することを特徴とする請求項23記載のリモートアクセスクライアント。

【請求項25】 前記端末離脱の検出において、前記管理テーブルに記録された接続中の各端末に対して所定時間毎に監視メッセージを送信し、該当端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項23記載のリモートアクセスクライアント。

【請求項26】 前記監視メッセージはOSIのレイヤ3アドレスを含み、前記応答メッセージはOSIのレイヤ2アドレスを含むことを特徴とする請求項25記載のリモートアクセスクライアント。

【請求項27】 前記端末離脱が検出されると、前記管理テーブルの当該端末に関する情報を削除することを特徴とする請求項23記載のリモートアクセスクライアント。

【請求項28】 1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANシステムで用いられるリモートアクセス方法であって、いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とするリモートアクセス方法。

【請求項29】 前記端末離脱の検出において、接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッシュホールド値を超えた時、当該端末が離脱したと判定することを特徴とする請求項28記載のリモートアクセス方法。

【請求項30】 前記端末離脱の検出において、当該リモートネットワークに接続中の各端末に対して所定時間毎に監視メッセージを送信し、該当端末から応答メッセージが返送されない場合に当該端末が離脱したと判定することを特徴とする請求項28記載のリモートアクセス方法。

【請求項31】 前記監視メッセージはOSIのレイヤ3アドレスを含み、前記応答メッセージはOSIのレイ

ヤ2アドレスを含むことを特徴とする請求項30記載のリモートアクセス方法。

【請求項32】 コンピュータに請求項28～31いずれかに記載の方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 LANの有する利便性の1つである端末の移動をインターネットもしくはイントラネットを利用した広域のLAN環境においても実現するには、当該端末のネットワーク内での接続位置を特定する必要がある。このためには端末の接続と離脱の検出が必要となる。本発明は、このうち端末離脱の検出を実現する技術に関する。

【0002】

【従来の技術】 複数のサブネットワークが接続されたインターネットもしくはイントラネットにおいて、端末が移動しうる環境（仮想LANシステム）を作ろうとすると、端末を収容するルータ等に端末の接続位置を管理する端末管理テーブルを設けてこのテーブルを端末の移動に合わせて自動更新する機能が必要である。このような機能を有する装置をクライアントと呼ぶ。

【0003】 上記のようなクライアントを有する仮想LAN制御システムの一形態例を図1に示す。図1中、10、20、30はインターネット上で仮想LANを構築するサブネットワークをそれぞれ備えたオフィス、40はインターネットである。なお、本発明はイントラネット等の同様のグローバルなパケット網に適用可能である。オフィス10は着目している端末101、102が通常、接続されるサブネットワーク（以下、ホームネットワークと称し、“HNW”と略称する）200を備えており、以後、ホームオフィスと呼ぶものとする。HNW200には仮想LANを構成するためのリモートアクセスサーバ（以下、“RAS”と略称する）301が接続されており、また、ルータ400を介してインターネット40に接続されている。

【0004】 また、オフィス20及び30は前記端末101、102が移動した時に接続されるサブネットワーク（以下、リモートネットワークと称し、“RNW”と略称する）501、502をそれぞれ備えており、以後、リモートオフィス20及び30と呼ぶものとする。RNW501及び502には仮想LANを構成するためのリモートアクセスクライアント（以下、“RAC”と略称する）601及び602がそれぞれ接続されており、また、ルータ400を介してインターネット40に接続されている。また、インターネット40にはルータ400を介して仮想LANを管理するための仮想LAN管理サーバ（以下、“IMS”と略称する）700が接続されている。

【0005】 ここで、パケットの（アドレス）構成例を

図9に示す。図において、1001がデータ、1002がレイヤ2アドレス、1003がレイヤ3アドレスを示す。それぞれのアドレスは発信と受信の2つのアドレスから構成される。詳しくはOSIのレイヤ2はフレーム、レイヤ3はパケットと呼ばれるが、ここでは転送単位という意味でいずれについてもパケットと呼ぶ。パケット網においては、リンクレベルとネットワークレベルでそれぞれ異なるアドレスが付与される。レイヤ2アドレス1002はMACアドレスとして知られており、端末製造時にベンダにより付与され、すべての端末を一意に識別できる情報である。一方、レイヤ3アドレス1003はIPアドレスとして知られており、ネットワークレベルでの個々の端末を識別するために付与され、接続位置に対して固定的に付与され、パケットのルーチングに利用される。

【0006】パケット網における端末間でのパケット転送例を図10に示す。111から114までが端末、401と402がルータ、800が通信経路である。この例では、端末111には、レイヤ2アドレス#1、レイヤ3アドレス#1が付与されている。図10中の矢印は、端末112から端末113にパケットが転送される状態を示す。端末112がパケットを送信すると、コリジョン（衝突）ドメイン内の全端末である端末111と端末112、そしてルータ401に対してパケットがブロードキャストされる。各々の受け取り先では、パケットの着レイヤ2アドレスと自身のレイヤ2アドレスとの照合が行われる。一致すればパケットを取り込み、不一致の場合にはパケットを廃棄する。ここでは、ルータ401がパケットを受信することになる。

【0007】ルータ401には、パケットの着レイヤ3アドレスと経路情報の対応表すなわちルーチングデータがあらかじめ保持されており、これに基づいてパケットの経路制御を実施する。この例では、通信先の端末113は経路800に接続されているため、パケットを経路800にルーチングする。このようにして最終的にはパケットは端末113に転送される。

【0008】図11は、パケット網に関して知られているアドレス解決法を説明するための図である。図において、401はルータ、111と112はルータ401の接続配下にある端末、900はルータ401が保持するARP（Address Resolution Protocol）キャッシュである。このARPキャッシュは、通信先のレイヤ2アドレスとレイヤ3アドレスの対応を管理するためのメモリである。通信先のレイヤ3アドレスは分かるがレイヤ2アドレスが不明の場合、ARPキャッシュを利用してレイヤ2アドレスを取得する方法がARPとして知られている。

【0009】ルータ401は、端末111のレイヤ2アドレスを取得しようとする場合、端末111のレイヤ3アドレスを設定したARP要求パケットを接続配下の全

端末に対してブロードキャストする。このARP要求パケットを受信した該当する端末（111）は、自身のレイヤ2アドレスを含むARP応答パケットを返送する。ルータ401は、このARP応答パケットからレイヤ3アドレスを取り出してARPキャッシュ900に保持し、以後の通信に用いる。なお、このARPキャッシュ900の内容は、一定時間保持された後消去される。

【0010】次に、図2は仮想LANの初期情報管理テーブル50を示すもので、本テーブルはIMS700に初期設定され、以降、本テーブルを参照して仮想LANの構成を行う。本テーブルは全仮想LAN構成端末のMACアドレスとHNW200のRAS301のIPアドレスとの対応テーブルである。

【0011】図3は位置情報管理テーブル60を示すもので、本テーブルはIMS700及びRAS301に設定され、端末のMACアドレスと、端末が現在接続しているネットワークの位置情報であるRASあるいはRACのインターネットアドレス（IPアドレス）との対応関係を管理する。このテーブルにより、IMS700及びRAS301は端末の位置をリアルタイムに管理することができる。

【0012】図4はホームアドレス管理テーブル70を示すもので、本テーブルはRAC601、RAC602に設定され、リモートネットワークに接続中の端末のMACアドレスと、該端末のホームアドレスであるRAS301のIPアドレスとの対応関係を管理する。このテーブルにより、RAC601、RAC602は端末から送出されたパケットをHNW200に転送することができる。

【0013】図5は図1のシステムにおける自動認証シーケンスを示すものである。以下、図1の構成を例にとり、本システムにおける自動認証及び位置管理（移動時）の原理をこのシーケンスに従って説明する。まず、端末101がHNW200からRNW501に移動する場合について説明する。

【0014】HNW200の端末101がRNW501に移動した後、端末102宛に最初のパケット（MACフレーム）を送出する場合（ステップS1、以下“ステップ”は省略）、RNW501上に接続されたRAC601は前記パケットを獲得し、このパケット（MACフレーム）における送信元端末101のMACアドレスを抽出し、該MACアドレスが認証済みかどうかホームアドレス管理テーブル70によりチェックする（S2）。

【0015】ここではホームアドレス管理テーブル70にエントリがないため（未認証）、IMS700にTE101のMACアドレスとRAC601のIPアドレスを送出して該端末101の認証要求を出す（S3）。IMS700はRAC601からの認証要求に対して、送られてきた端末101のMACアドレスをもとに、仮想LANシステム構築時に作成した上述した初期情報管理

テーブル50により、認証及びホームアドレス解決を行う。

【0016】即ち、端末101のMACアドレスが初期情報管理テーブル50に存在すれば(S4)、RAS301に対して認証OK及びHNW200のRAS301のIPアドレスを返す(S5)。そして、IMS700は移動した端末101の位置情報管理テーブル60を更新するとともに(S6)、移動した端末101のHNW200のRAS301に対して、端末101のインターネット上の位置情報に相当するRAC601のIPアドレスを位置情報通知として送る(S7)。

【0017】RAS301は、自分の管理する端末の位置情報を位置情報管理テーブル60上で更新する(S8)。RAC601はIMS700からの認証応答により、ホームアドレス管理テーブル70を作成し、端末101のホームアドレスに相当するRAS301のIPアドレスを登録する(S9)。これにより認証及びアドレス解決が終了する。一方、端末101のMACアドレスが初期情報管理テーブル50に存在しなければ、認証NGをRAC601に返す(S10)。RAC601はIMS700からの認証NGにより、端末101から送出されるパケットを廃棄する(S11)。

【0018】図6は、前述した自動認証が終了した後、ホームネットワークに自動接続する場合のシーケンス例(端末101から端末102へのデータ送信)である。以下、本システムにおける自動接続及びマルチプロトコル対応の接続の原理をこのシーケンスに従って説明する。端末101が移動した先のリモートネットワークのRAC601は、端末101から(端末102宛の)パケット(MACフレーム)が送られてくると(S21)、該端末が認証済みかどうかをホームアドレス管理テーブル70によりチェックし、認証済みであることを確認する(S22)。

【0019】次に、ホームアドレス管理テーブル70をもとに、端末のホームネットワークのRAS301に対して、端末101から送出されたパケットに対し、着IPアドレス(DA)をRAS301、発IPアドレス(SA)をRAC601としたIPヘッダ情報を付加してカプセル化し(S24)、RAC601よりRAS301に送信する(S24)。

【0020】RAS301では、送られてきた、IPヘッダ情報が含まれたパケットをデカプセル化し(S25)、HNW200上に送出する。これにより、移動した端末101はあたかもHNW200内でパケットを送ったように、RNW501からHNW200に接続されたTE102へパケット(MACフレーム)を送出することが可能となる(S26)。また、MACフレームをカプセル化することにより、OSIのレイヤ3以上のプロトコルに依存しない接続(即ち、マルチプロトコル)が可能となる。

【0021】一方、HNW200上の端末102から、移動した端末101に対して送信する場合を図7に示す。この場合、端末102から送出されたパケット(MACフレーム)をRAS301がモニタする(S31)。次に、位置情報管理テーブル60により到着先MACアドレスの位置をチェックし(S32)、移動した端末101のMACアドレスである場合はモニタしたパケットに対し、着IPアドレス(DA)を移動先のRAC601、発IPアドレス(SA)をRAS301としたIPヘッダ情報を付加してカプセル化し(S33)、RAS301よりRAC601に送信する(S34)。RAC601では、送られてきた、IPヘッダ情報が含まれたパケットをデカプセル化し(S35)、RNW501上に送出することにより、移動した端末101にパケットが届けられる(S36)。

#### 【0022】

【発明が解決しようとする課題】このような仮想LAN制御システムにおいて、端末が任意の場所に移動できるようにするには、端末の接続位置を特定する必要がある、このためには端末の離脱の検出が必要となる。従来、これは端末を離脱するときに端末の利用者がこれから離脱する旨の指示を行い、この結果をクライアントに通知する方法で実現していた。この方法では端末に特別な機能を設けることが必要となり、市販の端末がそのまま利用できないという問題があった。本発明は、上記の問題を解決するために、端末に特別な機能を設けることなく端末の離脱検出を実現することを目的とする。

#### 【0023】

【課題を解決するための手段】上記課題を解決するために、本発明は、1つ以上の端末が通常時接続されるホームネットワークと、前記端末が移動時に接続される少なくとも1つのリモートネットワークとがグローバル・ネットワークを介して接続された仮想的なLANにおいて、

- ・前記ホームネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、接続中の各端末の接続位置を示す管理テーブルを具備して、端末が前記リモートネットワークの1つに移動した時に該端末と前記ホームネットワークとのアクセスを、該端末が前記ホームネットワーク内でアクセスしているかのように制御するリモートアクセスサーバと、

- ・前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントと、

- ・前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートアクセスサーバの対応関係及び、接続中の各端末

の接続位置を示す管理テーブルを具備して、端末の接続位置及びパケット送信を管理する仮想LAN管理サーバとを有し、いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、前記仮想LAN管理サーバを介して端末離脱に伴うシステムの管理内容変更の制御を行う端末離脱検出システムを提供するものである。

【0024】また、本発明は、上記のような仮想的なLANシステムにおいて、いずれかの端末が前記少なくとも1つのリモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミングまたは該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出する端末離脱検出方法を提供する。

【0025】前記端末離脱検出の好ましい方法として、以下のような方法がある。

(1) 各リモートネットワークに接続中の各端末がパケットを送出する毎に、自動的にタイマ値が増加する監視タイマをその端末用にセットし、該タイマ値が所定のスレッショールド値を超えた時に当該端末が離脱したと判定する。

(2) 端末が接続管理下の第1のリモートネットワークから第2のリモートネットワークに移動した場合、当該端末のパケットの送出を検出し、当該端末の管理情報から該端末がそれまで接続していたリモートネットワークが前記第1のリモートネットワークであることを認識し、該第1のリモートネットワークのリモートアクセスクライアントに該端末の離脱を通知する。

(3) 前記リモートネットワークに接続中の各端末に対して所定時間毎に監視パケットを送信し、当該端末から応答パケットが返送されない場合に当該端末が離脱したと判定する。

【0026】(1)の方法では、端末が離脱後に一定時間経過すれば、必ず端末離脱が検出できる。

(2)の方法では、端末が第1のリモートネットワークから第2のリモートネットワークに移動してパケットを送出すると直ちに離脱を検出できる。

(3)の方法は、通常のARP手法による監視パケットの送出を利用して実現できる。また、これらの方法を組み合わせても良い。

【0027】また、本発明は、上記仮想LAN制御システムにおける、対応する機能を有する仮想LAN管理サーバ、即ち、前記グローバル・ネットワークに接続され、該グローバル・ネットワークのアドレスを有し、各端末と前記リモートネットワークのリモートアクセスサーバの対応関係及び、接続中の各端末の接続位置を示す

管理テーブルを具備して、端末の接続状態及びパケット送信を管理する仮想LAN管理サーバを提供するものであり、ここで、いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が更に他のリモートネットワークに移動した場合の接続情報に基づいて当該端末の当該リモートネットワークからの離脱を検出し、端末離脱に伴うシステムの管理内容変更の制御を行うことを特徴とする。

【0028】更に、本発明は、上記仮想LAN制御システムにおける、対応する機能を有するリモートアクセスクライアント、即ち、前記各リモートネットワークに接続され、前記グローバル・ネットワークのアドレスを有し、該リモートネットワークに接続中の各端末と前記ホームネットワークとの対応関係を示す管理テーブルを具備して、前記リモートネットワークと前記グローバル・ネットワークとの通信を制御するリモートアクセスクライアントを提供するものであり、ここで、いずれかの端末が前記リモートネットワークの1つに接続され管理されている場合、該端末が送出するパケットのタイミング情報に基づいて当該端末の当該リモートネットワークからの離脱を検出することを特徴とする。

【0029】また、本発明は、これらサーバやクライアントに対応する方法及び、それら方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記憶媒体を提供するものである。

【0030】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態について説明する。以下の説明において、仮想LAN制御システムの基本構成は、上述した図1の構成と同一である。

【0031】図8は、本発明による端末離脱シーケンスの一例であり、RNW501に移動した端末101が再びHNW200に移動する際の例である。RAC601では端末101がパケット(MACフレーム)を送出する毎に(S41)、時間の経過に合わせて自動的にタイマ値が増加する端末離脱監視タイマをリセットし(S42)、このタイマ値があるスレッショールド値をこえた時(S43)、RNW501より離脱したとみなす(S44)。このタイマの利用により、端末側のプロトコルに依存しないマルチプロトコル対応の離脱が可能となる。RAC601ではタイムアウトを検出すると、IMS700に対し、端末が離脱したことを示す端末離脱要求パケットを送出する。該パケットの内容は、TE101のMACアドレスとRAC601のIPアドレスを有したものととなっている(S45)。

【0032】IMS700では該パケットを受信すると、位置情報管理テーブル60の端末101に関する内容を、端末101が移動していたリモートネットワークのRAC601のIPアドレスから、端末101のデフォルト位置であるHNW200のRAS301のIPア



ドレスに更新する(S46)。また、RAC601には端末離脱応答パケットを送出し(S47)、RAS301には端末101のMACアドレスとRAC601のIPアドレスを付けて端末離脱通知を送出する(S48)。

【0033】RAC601では、端末離脱応答をIMS700から受信することによって、端末のホームアドレス管理テーブル70の該端末のエントリを削除することにより端末離脱処理を完了する(S49)。RAS301はIMS700からの端末離脱通知を受信すると、端末101の現在の接続位置を登録するために位置情報管理テーブル60を更新する(S50)。

【0034】この方法によれば、端末が離脱した後で一定時間経過すれば必ず端末離脱が検出できる。そして、端末の位置を管理する管理テーブルが移動に合わせて自動更新されるので、端末がネットワーク間を移動しても環境の再設定は不要である。しかしながら、端末が通信する頻度と通信時間の特性を考慮してどの端末にも当てはまるようにスレッショルド値を決めるため、端末離脱の検出に遅れが出る可能性がある。

【0035】図12に、本発明による端末離脱シーケンスの第2の例を示す。本実施例は、端末101がRNW501からRNW502に移動する場合の例である。端末101がRNW502に移動後にパケットを送信すると(ステップS61)RAC602がこれを検出し、端末101が接続したことを通知する端末接続通知パケットをIMS700に送出する(ステップS62)。IMS700では、このパケットを受信すると、位置情報管理テーブル60を検索して端末101が移動したこと、そして移動前まで接続していたRNWが501であることを認識する(ステップS63)。そして、端末101が移動したことを示す端末離脱通知パケットをRAC601に通知する(ステップS64)。

【0036】RAC601はこのパケットを受信すると端末101が離脱したことを知り、自身のホームアドレス管理テーブル70の端末101に関する情報を削除し、離脱処理を行う(ステップS65)。同時に、IMS700は、端末101が移動したことを示す端末接続位置通知パケットをRAS301に通知する(ステップS66)。この方法では、端末が移動(離脱)後に通信を行おうとするまでは離脱が検出できないが、通信を開始すると離脱が直ちに検出できるという長所を有する。上記第1と第2の例に示すいずれかの方法のみで離脱を検出しても良いし、両方の方法を併用して検出しても良い。2つの方法を併用することにより、端末離脱がより正確に検出できる。

【0037】2つの方法を併用したシーケンス例を図13に示す。本例もまた、RNW501にそれまで接続され通信していた端末101がRNW502に移動し通信を開始した場合である。即ち、RNW501にそれまで

接続されていた端末101がRNW502に移動後に通信を行おうとしてパケットを送信すると(ステップS71)、RAC602がこれを検出し、自身のホームアドレス管理テーブル70を検索するが、ここでは端末101についてのレコードがないため、RAC602は端末101が新たに接続されたことを知る(ステップS72)。

【0038】RAC602は、端末101のMACアドレスと自身の識別情報(IPアドレス)を含む端末接続通知パケットをIMS700に送信する(ステップS73)。IMS700はこのパケットを受信すると、パケットに含まれた情報に基づいて自身の初期情報管理テーブル50を検索する(ステップS74)。端末101はこのテーブルに関しては登録済みであるため、IMS700は、端末101が認証されたことをRAC602に通知し(ステップS75)、RAC602は、自身の管理テーブル70に端末101のレコードを追加する(ステップS76)。また、同時に、IMS700はRAS301に、端末101の新たな接続位置を示す端末接続位置通知パケットを送信する(ステップS77)。

【0039】RAS301はこのパケットを受信すると、自身の位置情報管理テーブル60の端末101の接続位置に関するデータを更新する(ステップS78)。一方、IMS700側では、管理テーブル60を検索すると端末101はそれまでRAC601に接続されていたことが分かるので、RAC601に端末離脱通知パケットを送信する(ステップS79)。RAC601はこのパケットを受信すると自身の管理テーブル70から端末101に関するレコードを削除し、端末離脱処理を行う(ステップS80)。

【0040】一方、RAC601が保持する端末101に関する端末離脱監視タイマは、端末101から最後のパケットを受信した時点からタイマ値が時間の経過に合わせて増加する。そのため、一定時間経過するとこのタイマがタイムアウトし、端末離脱が検出される(ステップS81)。この結果、RAC601は自身の管理テーブル70から端末101に関するレコードを削除し端末離脱処理を行う(ステップS80)。

【0041】従って、RAC601は、端末離脱通知パケットの受信もしくは端末離脱監視タイマのタイムアウトのいずれか早い方の情報で端末101の離脱が検出できる。即ち、端末が離脱後通信を再開しなくても一定時間経過すると端末離脱監視タイマを利用する第1の方法で、一方、端末が離脱後早い時期に新たなRNWで通信を再開した場合には第2の方法で端末離脱を検出できる。このように2つの方法を併用すると、より正確に端末離脱が検出でき、また、もちろんこの場合も端末に特別な機能を設ける必要はない。

【0042】図14に、本発明による端末離脱シーケンスの第3の例を示す。本例は、端末の離脱の検出を、上



述したARPの手法を応用して実現しようというものである。本例は、端末101がHNW200からRNW501に移動して通信を行おうとする場合の例である。端末101が移動後に新たに第1の packets を発信すると（ステップS91）、packets 送出を検出したRAC601は自身の管理テーブル70を検索する。ここで、端末101に関する登録情報は見つからないため、RAC601はIMS700に端末認証要求 packets を送信する（ステップS92）。この packets は端末101のMAC（レイヤ2）アドレスと要求元RACの識別情報（IPアドレス）を含む。

【0043】IMS700では、この packets に含まれたMACアドレスから初期情報管理テーブル50を検索して端末101が登録済み端末であることを認証する（ステップS93）。また、位置情報管理テーブル60を検索して端末101の接続位置がHNW200からRNW501に移動したことを知り、端末101の新たな接続先を管理するために、テーブル60の該当レコードを更新する（ステップS94）。そして、認証結果 packets をRAC601に返送する（ステップS95）。

【0044】この packets により端末101は登録済みであることが認証されたため、RAC601では、当該 packets の内容に基づいて自身の管理テーブル70に端末101のMACアドレス情報を追加する（ステップS96）。次に、端末101が第2以降の packets を転送すると（ステップS97）、RAC601はこのテーブル70の情報を用いてこれを認証し、packets を中継する（ステップS98）。

【0045】RAC601は、自身の管理テーブル70に記録されている各端末に対して、所定の時間毎に、端末のIP（レイヤ3）アドレスを設定し、そのMAC（レイヤ2）アドレスを問い合わせる監視 packets を送信する（ステップS99）。即ち、端末101に対しても監視 packets が送信されるが、この監視 packets の着信IPアドレスは端末101に設定されているので、端末101がRNW501から離脱すると（ステップS100）、予期される応答 packets が返送されない。

【0046】一定時間経てもRAC601に応答 packets が返送されない場合、RAC601は端末101は離脱したものと判断する（ステップS101）。この場合、自身の管理テーブル70の該当レコードを削除する（ステップS102）とともに、IMS700に端末離脱通知 packets を送信する（ステップS103）。IMS700は、端末離脱通知 packets を受信すると自身の位置情報管理テーブル60内の端末101に関するレコードの現在の接続位置をデフォルト位置であるHNW200のRAS301のIPアドレスに変更する（ステップS104）。更に、IMS700は、端末101のHNWのRAS301に端末離脱通知 packets を送信する（ステップS105）。RAS301もまた、自身の位

置情報管理テーブル60の内容を、端末101の移動に合わせ更新する（ステップS106）。

【0047】即ち、この例の場合、端末101の離脱後一定時間経ると、ARP手法を利用した監視 packets （及び応答 packets ）により離脱が検出できる。即ち、RAC、RAS、IMS側に端末の移動を自動検出する機能を設けることにより、端末に特別な機能を設けなくても端末離脱が検出できる。

【0048】

10 【発明の効果】即ち、本発明によれば、仮想LAN制御システムにおいて端末が任意の場所に移動できるようにするために必要な端末離脱の検出が、端末に特別なシステムや手順を設定することなく実現できる。

【図面の簡単な説明】

【図1】 本発明に関する仮想LAN制御システムの構成例である。

【図2】 初期情報管理テーブルの一例を示す図である。

【図3】 位置情報管理テーブルの一例を示す図である。

【図4】 ホームアドレス管理テーブルの一例を示す図である。

【図5】 本仮想LAN制御システムにおける自動認証シーケンスを示す図である。

【図6】 本システムにおける自動接続シーケンス例を示す図である。

【図7】 本システムにおける自動接続シーケンス例を示す図である。

【図8】 本発明による自動離脱シーケンス例を示す図である。

【図9】 packets のアドレス構成例を示す図である。

【図10】 packets 転送例を示す図である。

【図11】 アドレス解決法の例を示す図である。

【図12】 本発明による自動離脱シーケンス例を示す図である。

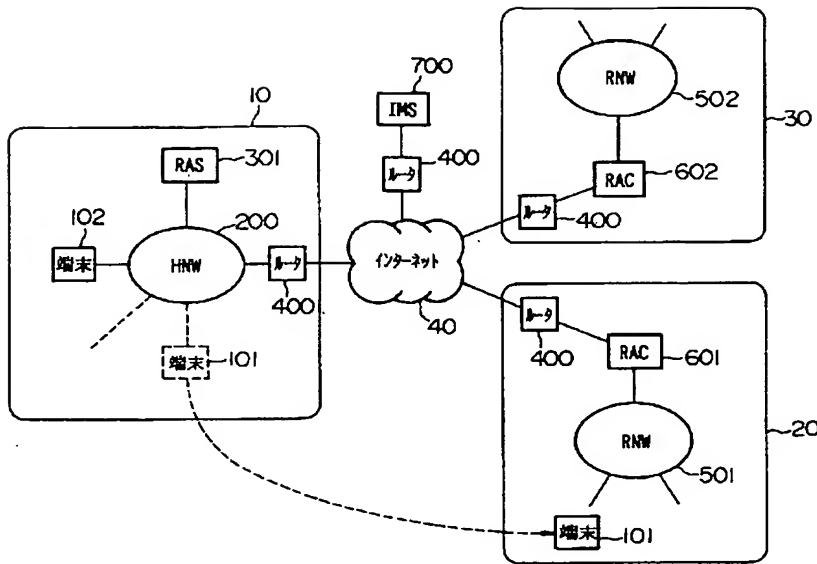
【図13】 本発明による自動離脱シーケンス例を示す図である。

【図14】 本発明による自動離脱シーケンス例を示す図である。

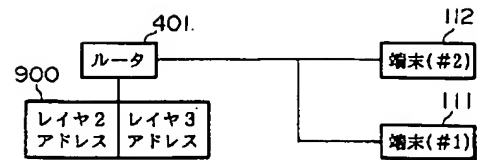
40 【符号の説明】

10…ホームオフィス、20、30…リモートオフィス、40…インターネット、50…初期情報管理テーブル、60…位置情報管理テーブル、70…ホームアドレス管理テーブル、200…HNW（ホームネットワーク）、501、502…RNW（リモートネットワーク）、301…RAS（リモートアクセスサーバ）、601、602…RAC（リモートアクセスクライアント）、101、102…端末、700…IMS（仮想LAN管理サーバ）、400…ルータ。

【図1】



【図11】



【図2】

端末のMACアドレス	端末のホームネットワークアドレス (RASのIPアドレス)
端末101のMACアドレス	RAS301のIPアドレス
端末102のMACアドレス	RAS301のIPアドレス
⋮	⋮

50

【図3】

端末のMACアドレス	端末の位置情報 (RAS or RACのIPアドレス)
端末101のMACアドレス	RAS301のIPアドレス
端末102のMACアドレス	RAS301のIPアドレス
⋮	⋮

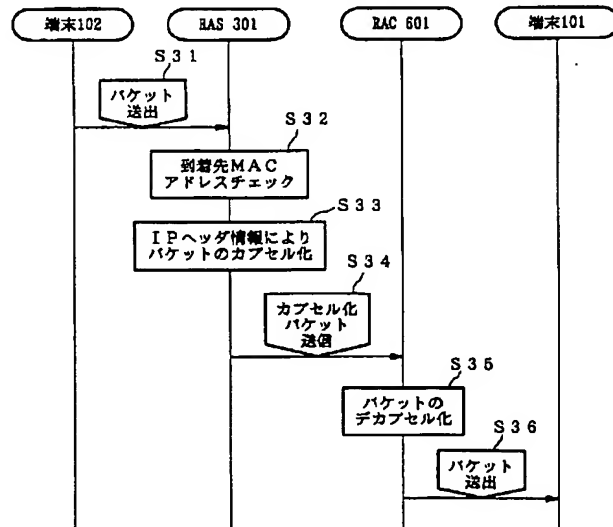
60

【図4】

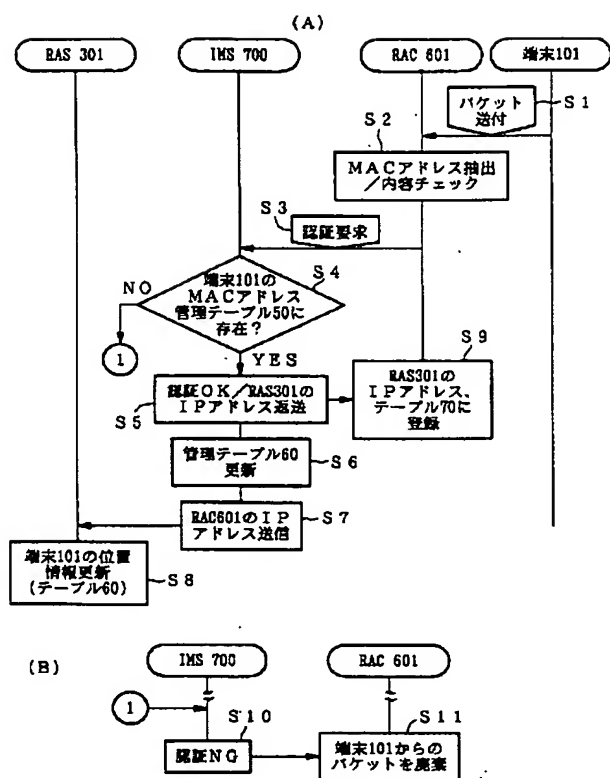
移動端末のMACアドレス	移動端末のホームアドレス (RASのIPアドレス)
端末101のMACアドレス	RAS301のIPアドレス
⋮	⋮

70

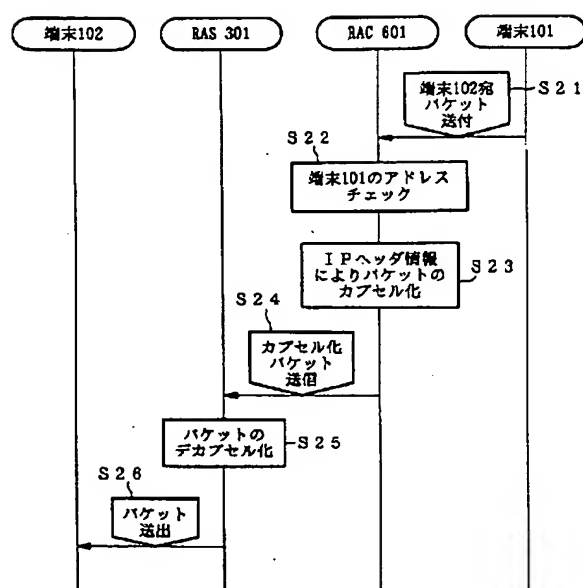
【図7】



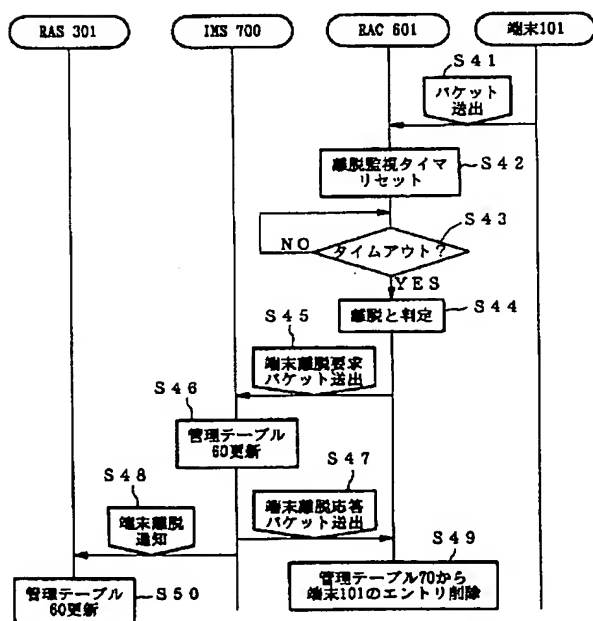
【図5】



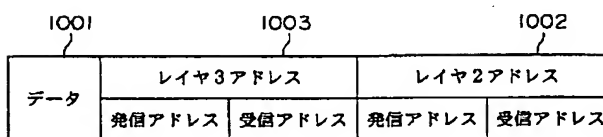
【図6】



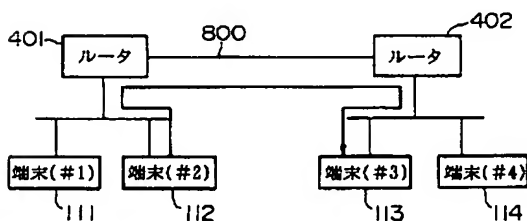
【図8】



【図9】



【図10】



```

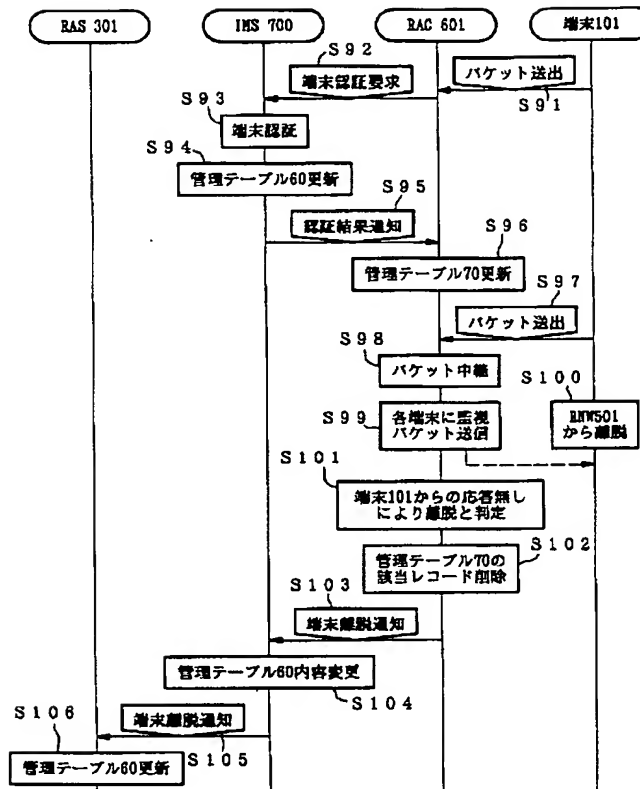
sequenceDiagram
    participant RAS301 as RAS 301
    participant RAC601 as RAC 601
    participant IMS700 as IMS 700
    participant RAC602 as RAC 602
    participant End101 as 端末101

    End101->>RAC602: S 6 1  
パケット  
送出
    RAC602->>IMS700: S 6 2  
端末接続  
通知
    IMS700->>RAC601: S 6 3  
端末101の移動  
と移動前の  
接続先を伝達
    RAC601->>RAC602: S 6 4  
端末離脱  
通知
    RAC602->>RAC601: S 6 5  
端末離脱処理
    RAC601->>RAS301: S 6 6  
端末接続  
位置通知
  
```

The diagram illustrates the sequence of operations for packet transfer and terminal management across five entities: RAS 301, RAC 601, IMS 700, RAC 602, and 端末101 (Terminal 101). The process begins with Terminal 101 sending a packet (S 6 1) to RAC 602. RAC 602 then sends a terminal connection notification (S 6 2) to IMS 700. IMS 700 relays this information to RAC 601 as a notification of terminal 101's movement and previous connection (S 6 3). RAC 601 then sends a terminal disconnection notification (S 6 4) back to RAC 602. RAC 602 performs a terminal disconnection process (S 6 5) and finally sends a terminal connection position notification (S 6 6) to RAS 301.

[illegible]

【図14】



フロントページの続き

(72)発明者 増井 貴

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 永井 浩一

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内